REMARKS

Claims 1-15 were pending in the patent application. By this amendment, Claim 14 is canceled and amendments are introduced for Claims 1, 4, 5, 9, 11, and 12. The Examiner has stated that the drawings are objected to; and, has finally rejected Claims 1-15 under 35 USC 102 as anticipated by the Gibbs patent. Applicants submit herewith new drawings and claims' amendment. For the reasons set forth below, Applicants believe that the claims, as amended, are patentable over the Gibbs patent.

The present invention teaches and claims a signature device, such as a chipcard, which includes a signature program and additional signature certificate information for providing an expanded electronic signature to sign a document (page 6, lines 16-22). The signature device executes the signature program and does not require that an external authenticating entity generate the digital signature when the user is attempting to digitally sign a document ("the external and internal information together with the hash are merged on the chipcard 101", from page 13, line 14; "merger is effected by the chipcard program", from page 13, line 18; and, "[t]his encryption takes place on the chipcard", from page 14, lines 11-12). The digital signature includes at least one identifying characteristic for identifying the signature device which executed the signature program (see: page 3, lines 1-3; page 4, lines 1-4; page 13, lines 4-7; and page 15, lines 6-9) as well as a document extract value identifying the document which is being signed (see: page 12, lines 19-20; and page 14, lines 23-24). All of the independent claims, Claims 1, 9, 11, and 12 as amended, expressly recite that the signature device stores the signature program which is to be executed as well the necessary additional information so that it can perform digital signing of a document, and that the digital signing incorporates at least one identifying characteristic identifying the signature device which executed the program to sign the document as well as a document extract value for the document to be signed.

The Gibbs patent is directed to a server-based electronic "signature" system and method, whereby an authenticated message server receives requests for digital "signatures" and generates digital "signatures" in response to the requests. The requests which are received by the authenticated message server are actually requests to obtain access to services (see: Col. 7, lines 41-48). Accordingly, the server generates a "signature" which is sent to the requester and which allows that requester temporary or restricted privileges to the requested service (see: abstract, Col. 6, lines 46-56). The server maintains randomly-generated keys used to generate digital "signatures" (see: Col. 3, lines 50-52), counters for tracking how many "signatures" have been generated by a particular key (see: Col. 3, lines 55-58), and the process, or user interface, for performing authentication (Col. 3, lines 16-30). Under the Gibbs system, an authenticated message server creates all digital signatures for distribution to the requesters and the requesting entities do not have any capability of creating digital signatures. As explicitly taught by Gibbs, an "adapted digital signature" includes the signature along with information for contacting an authenticating server, specifically the service id and domain name (Col. 3, lines 16-30) so that authorization of the "signature" can be verified by the server. When a user seeks to use the digital signature, for example to obtain access to a restricted web page or to make a purchase, the user enters the "adapted digital signature" with signature component 132 and then a server process is contacted for authentication (see: Col. 8, lines 45-55 and Col. 9, lines 59-64).

Applicants respectfully contend that the Gibbs patent does not teach or suggest that a signature device having a signature program and certificate with signature key stored thereon dynamically, in situ, generates a digital signature to sign a particular document. Gibbs teaches that a server generates an access password and sends it to a user. Clearly, therefore, Gibbs does not anticipate the claimed method or apparatus for dynamically generating a digital signature for a document at the signature device, wherein the signature device includes the signature program and certificate.

Moreover, the Gibbs "signature"/access password does not include a document access value for a particular document to be signed. While Gibbs does teach that an index number is used along with a system key to derive an adapted digital "signature", the Gibbs index number is not a value which is unique to a document or service. It is an incremented value that "identifies one of a number of unique digital signatures generated for a particular system key...[and which is] periodically reinitialized by the authenticated message server 100..." (Col. 3, lines 50-62).

Applicants note that the Examiner has cited the teachings from Col. 2, lines 27-24 (*sic,* Applicants assume that the Examiner intended to cite "lines 27-34") against the claim language of "a document extract value of the document for signing". The cited teachings are directed to the authenticating server extracting a digital signature in order to authenticate the digital signature. Applicants respectfully assert that the cited passage does not include any teachings related to identifying a particular document. Moreover, extracting information from a communication effectively teaches away from the claim language which recites incorporating information into a digital signatures.

Applicants further assert that Gibbs does not teach or suggest that the digital "signature" includes any identifying information to identify the signature device which generated the digital signature. The Examiner has cited the passages found in Col. 3, lines 31-49; Col. 6 at lines 26-29; Col. 8, lines 38-55; and, Col. 9, lines 1-9 against the claim limitations regarding identifying the signature device. The cited passage from Col. 3 details the components of the Gibbs digital "signature" including the system key used to generate the signature. The system key, which is defined in Col. 3 at lines 50-52 as "...a 256 bit value that changes periodically and is randomly generated" does not, however, identify the signature device. With regard to the teachings cited from Col. 6, the cited passage teaches that the message server may include router functionality. There is nothing in the passage, however, which teaches or suggests information in the digital signature identifying the signature device. With regard to the passage from Col. 8, the cited teachings discuss sending a digital signature to a user and authenticating a digital signature. None of the teachings relate to a digital signature having information which identifies the signature device which generated the signature. Finally, the passage from Col. 9, lines 1-9 again discusses inclusion of the system key. As argued above, the system key is a changeable value which does not identify the signature device.

Applicants conclude, therefore, that the Gibbs patent does not anticipate the invention as claimed. It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Gibbs patent does not teach the signature device and method as claimed, including means and steps for a signature device, having a signature program and certificate, to generate a digital signature which identifies the signature device and uses a document extract value for the document to be signed, it cannot be maintained that the Gibbs patent anticipates the invention.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

E. Hamann, et al

By: Anne Vachon Dougherty

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910